Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

receiving, with a first processor, data for use in an operation in a second processor, the first processor being an applications processor including cryptographic and security capabilities that are excluded in the second processor, the second processor being a wireless communications processor;

verifying, with the first processor, a credibility of the data for the second processor by validating that the data is sent from a trusted ~~source;~~source by public and private keys;

placing the first and second processors in a trusted state;

exiting the trusted state if the credibility of the data fails; and

initiating the operation with the second processor while the trusted state has not been exited.

2. (Original) The method of claim 1, wherein the operation comprises an information update.

3. (Previously Presented) The method of claim 2, further comprising:

setting a register containing a value using the first processor when exiting the trusted state.

4. (Previously Presented) The method of claim 3, further comprising reading the value using the second processor.

5. (Previously Presented) The method of claim 3, further comprising preventing an execution of the operation if the value is not indicative of the trusted state.

6. (Previously Presented) The method of claim 3, further comprising initiating remediation if at least the value is not indicative of the trusted state.

7. (Previously Presented) The method of claim 2, further comprising receiving the information update via an air interface with the second processor and providing the information update to the first processor.

8. (Canceled)

9. (Currently Amended) A method comprising:

maintaining a hardware asset with an applications processor of a system to indicate to another hardware component of the system a trust state of the applications processor, the applications processor including cryptographic and security capabilities that are excluded in the other hardware component, wherein the system comprises a wireless device;

receiving, with the other hardware component, data for use in an operation in the other hardware component; and

verifying, with the applications processor, a credibility of the data for the other hardware component by validating that the data is sent from a trusted ~~source.~~source by public and private keys.

10. (Previously Presented) The method of claim 9, further comprising accessing the hardware asset using the other hardware component of the system.

11. (Canceled)

12. (Previously Presented) The method of claim 10, further comprising updating digital content in the other hardware component if the hardware asset indicates the trust state is valid.

13. (Previously Presented) The method of claim 10, further comprising preventing updating the other hardware component if the hardware asset does not indicate the trust state is valid.

14. (Previously Presented) The method of claim 13, further comprising performing a remediation measure using the other hardware component if the trust state is not valid.

15. (Previously Presented) The method of claim 13, further comprising providing an indication to the applications processor if an update was attempted when the trust state was not valid.

16. (Previously Presented) The method of claim 9, further comprising

setting the hardware asset via the applications processor when exiting a trusted state, wherein the hardware asset comprises a one-way register.

17. (Previously Presented) The method of claim 10, further comprising

determining if an update is trusted in the applications processor and transferring the update to the other hardware component if the hardware asset indicates the trust state is valid.

18. (Currently Amended) An apparatus comprising:

a hardware asset, maintained by an applications processor, to indicate a trust state of an application processor portion of the apparatus to a communications processor, the applications processor including cryptographic and security capabilities that are excluded in the second processor, the communications processor receiving data for use in an operation in the communications processor, the applications processor verifying a credibility of the data for the communications processor by validating that the data is sent from a trusted ~~source.~~source by public and private keys.

19. (Previously Presented) The apparatus of claim 18, wherein the hardware asset is accessible by the communications processor of a wireless device.

20. (Previously Presented) The apparatus of claim 19, wherein the communications processor cannot modify a value of the hardware asset.

21. (Previously Presented) The apparatus of claim 18, wherein the hardware asset is coupled to receive a program signal if the trust state of the applications processor portion is not valid.

22. (Original) The apparatus of claim 18, wherein the hardware asset is coupled to receive a reset signal to initiate a trusted state.

23. (Original) The apparatus of claim 18, wherein the hardware asset comprises a one-way register.

24. (Currently Amended) A system comprising:

a hardware asset to indicate a trust state of an applications processor portion of the system to a communications processor portion of the system, the applications processor portion including cryptographic and security capabilities that are excluded in the communications processor portion, the communications processor portion receiving data for use in an operation in the communications processor portion, the applications processor portion verifying a credibility of the data for the communications processor portion by validating that the data is sent from a trusted~~ source;~~source by public and private keys; and

a wireless interface coupled to the hardware asset.

25. (Previously Presented) The system of claim 24, wherein the hardware asset is accessible by the communications processor portion of the system, wherein the system comprises a wireless device.

26. (Original) The system of claim 24, wherein the hardware asset comprises a one-way register.

27. (Original) The system of claim 24, wherein the wireless interface comprises an antenna.

28. (Currently Amended) An article including a machine-accessible storage medium containing instructions that if executed enable a system to:

control a hardware asset of the system with an applications processor to indicate a trust state of an applications processor portion of the system to another hardware portion of the system, the applications processor portion including cryptographic and security capabilities that are excluded in the other hardware portion, wherein the system comprises a wireless device, the other hardware portion receiving data for use in an operation in the other hardware portion, the applications processor portion verifying a credibility of the data for the other hardware portion by validating that the data is sent from a trusted ~~source.~~source by public and private keys.

29. (Previously Presented) The article of claim 28, further comprising instructions that, if executed, enable the system to update the other hardware portion of the system if the hardware asset indicates the trust state is valid.

30. (Previously Presented) The article of claim 28, further comprising instructions that if executed enable the system to prevent or discard an update to the other hardware portion of the system if the hardware asset indicates the trust state is not valid.

31. (Previously Presented) The article of claim 30, further comprising instructions that if executed enable the other hardware portion to initiate a remediation operation if the hardware asset indicates the trust state is not valid.

32. (Previously Presented) The article of claim 28, further comprising instructions that, if executed, enable the system to perform a secure operation in the other hardware portion of the system if the hardware asset indicates the trust state is valid.

33. (Previously Presented) The article of claim 28, further comprising instructions that, if executed, enable the applications processor portion to vector into a trusted state before initiating a transfer operation to the other hardware portion of the system.

34. (Currently Amended) A method comprising:

receiving, with a communications processor portion of a system, data for use in an operation in the communications processor portion;

verifying, with an applications processor portion of the system, the applications processor portion including cryptographic and security capabilities that are excluded in the communications processor portion, a credibility of the data for the communications processor portion by validating that the data is sent from a trusted ~~source;~~source by public and private keys;

setting a value to indicate a trust state of the applications processor portion;

accessing the value with the communications processor portion; and

determining the trust state of the applications processor portion based on the value.

35. (Previously Presented) The method of claim 34, further comprising initiating an operation in the communications processor portion if the value is indicative of the trust state.

36. (Original) The method of claim 35, wherein the operation comprises an information update.

37. (Previously Presented) The method of claim 34, wherein the applications processor portion comprises an applications portion of a wireless device and the communications processor portion comprises a communications portion of the wireless device.